

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Microsoft's January 2024 Patch Tuesday Addresses 49 Vulnerabilities**

Date of Publication

January 10, 2024

Admiralty Code

A1

TA Number

TA2024010
















# Summary
















**First Seen:** January 9, 2023

**Affected Platforms:** Windows Kerberos, Windows Hyper-V, Windows HTML Platforms, Microsoft Common Log File System, Windows Win32K, Windows Kernel, Microsoft Remote Desktop Client, Windows Cloud, Microsoft SharePoint, and more

**Impact:** Denial of Service (DoS), Elevation of Privilege (EoP), Information Disclosure, Remote Code Execution (RCE), Security Feature Bypass, and Spoofing

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20674	Windows Kerberos Security Feature Bypass Vulnerability	Windows Kerberos			
CVE-2024-20700	Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V			
CVE-2024-20652	Windows HTML Platforms Security Feature Bypass Vulnerability	Windows HTML Platforms			
CVE-2024-20653	Microsoft Common Log File System Elevation of Privilege Vulnerability	Microsoft Common Log File System			
CVE-2024-20683	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32k			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20686	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32k			
CVE-2024-20698	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel			
CVE-2024-21307	Remote Desktop Client Remote Code Execution Vulnerability	Microsoft Remote Desktop Client			
CVE-2024-21310	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud			
CVE-2024-21318	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint			

# Vulnerability Details

## #1

Microsoft's January 2024 Patch Tuesday includes security updates for a total of 49 vulnerabilities, comprising two critical and 47 important severity vulnerabilities. The breakdown of vulnerabilities includes 10 Elevation of Privilege, 12 Remote Code Execution, 11 Information Disclosure, 7 Security Feature Bypass, 6 Denial of Service, and 3 Spoofing vulnerabilities.

## #2

The updates cover various Microsoft products such as Office, SQL Server, .NET, Visual Studio, Windows Scripting, .NET Framework, Windows TCP/IP, Windows Win32K, Windows Kernel, and Windows Hyper-V. Notably, Microsoft patched four vulnerabilities in the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 53. None of the vulnerabilities addressed in this release were reported to be actively exploited in the wild. This advisory pertains to 10 CVEs that could potentially be exploited.

## #3

One of the critical patches, CVE-2024-20674, addresses a Windows Kerberos Security Feature Bypass Vulnerability, which could potentially enable an unauthenticated attacker to conduct a machine-in-the-middle attack, spoofing a Kerberos server. This vulnerability has the highest Common Vulnerability Scoring System (CVSS) rating for the month, and Microsoft expects public exploit code to emerge within 30 days.

## #4

The second critical patch, CVE-2024-20700, addresses a Windows Hyper-V Remote Code Execution Vulnerability. Although labeled as 'remote,' the execution is network adjacent, and Microsoft does not provide specifics on how the code execution occurs. Notably, no authentication or user interaction is required for this vulnerability, adding to its attractiveness for potential exploitation.

## #5

Other notable vulnerabilities include elevation of privilege flaws in Win32k and Windows Kernel, a remote code execution vulnerability in a Remote Desktop Client, a security feature bypass in Internet Explorer, and elevation of privilege vulnerabilities in Microsoft Common Log File System and Windows Cloud Files Mini Filter Driver. Successful exploitation of some of these vulnerabilities could allow attackers to gain SYSTEM privileges. The release emphasizes the importance of promptly applying the updates to mitigate potential security risks.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20674	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-254
CVE-2024-20700	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-362
CVE-2024-20652	Windows: 10 - 11 23H2 Windows Server: 2003 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-254

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20653	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-264
CVE-2024-20683	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-264
CVE-2024-20686	Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows_server_2022_23h2:*:*:*:*:*:*	CWE-264
CVE-2024-20698	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-264
CVE-2024-21307	Windows: 10 - 11 23H2 Windows Server: 2008 R2 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-362
CVE-2024-21310	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-264
CVE-2024-21318	Microsoft SharePoint Server: 2016, 2019, Subscription Edition	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*	CWE-264



# Recommendations



Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.



Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.



Prioritize critical vulnerabilities, especially CVE-2024-20674 (Windows Kerberos Security Feature Bypass) and CVE-2024-20700 (Windows Hyper-V Remote Code Execution). These vulnerabilities have the potential for severe exploitation and should be addressed urgently.



Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.



Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

## Potential **MITRE ATT&CK** TTPs

<b>TA0004</b> Privilege Escalation	<b>TA0042</b> Resource Development	<b>TA0007</b> Discovery	<b>TA0002</b> Execution
<b>TA0003</b> Persistence	<b>TA0006</b> Credential Access	<b>T1588</b> Obtain Capabilities	<b>T1588.005</b> Exploits
<b>T1059</b> Command and Scripting Interpreter	<b>T1588.006</b> Vulnerabilities	<b>T1068</b> Exploitation for Privilege Escalation	<b>T1203</b> Exploitation for Client Execution
<b>T1082</b> System Information Discovery	<b>T1557</b> Adversary-in-the-Middle	<b>T1036</b> Masquerading	<b>T1498</b> Network Denial of Service

## Patch Details

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20652>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20653>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20686>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318>

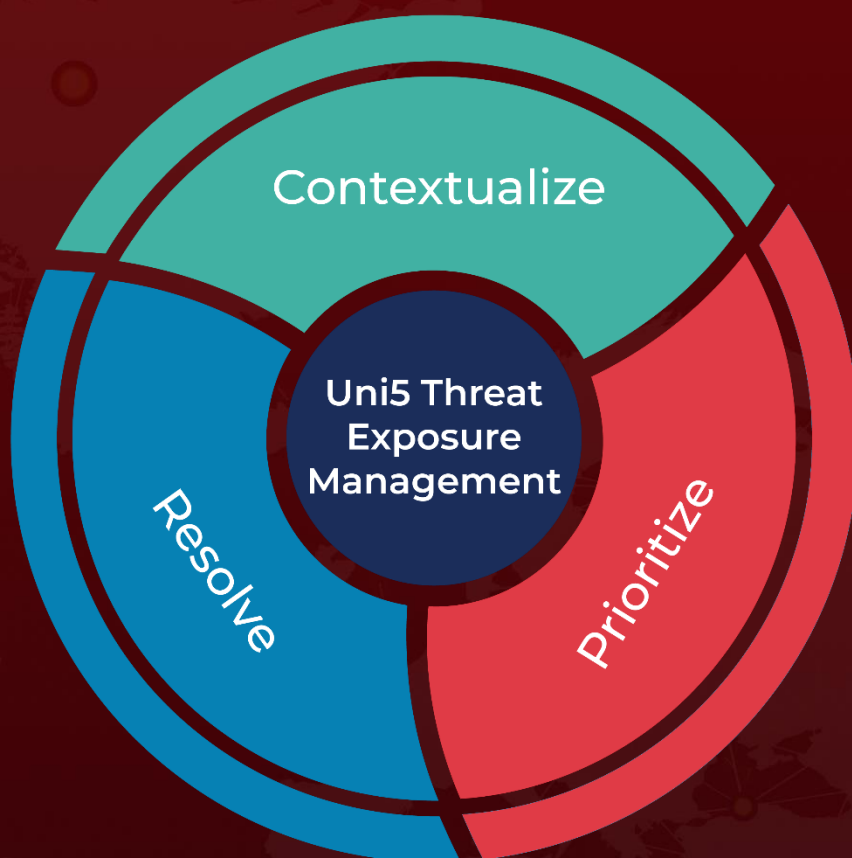
## References

<https://msrc.microsoft.com/update-guide/releaseNote/2024-Jan>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**January 10, 2024 • 5:30 AM**

© 2024 All Rights are Reserved by Hive Pro®



More at [www.hivepro.com](http://www.hivepro.com)